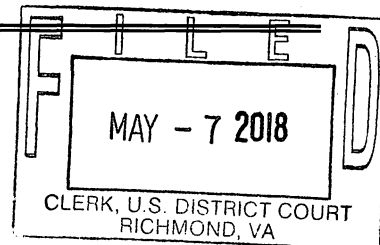


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia



In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

5300 GLENSIDE DRIVE
APARTMENT 1808
HENRICO, VIRGINIA 23228

Case No. 3:18SW92

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

as described in Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

items described in Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1029(a)	Fraud and related activity in connection with access devices
18 U.S.C. § 1028A	Aggravated identity theft

The application is based on these facts:

See attached affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jeremy D'Errico, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 05/07/2018

IS/
David J. Novak
United States Magistrate Judge

Judge's signature

City and state: Richmond, Virginia

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF:

**5300 GLENSIDE DRIVE
APARTMENT 1808
HENRICO, VIRGINIA 23228**

Case No. 3:18sw92

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR
A WARRANT TO SEARCH AND SEIZE**

I, **Jeremy A. D'Errico** being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 5300 Glenside Drive, Apartment 1808, Henrico, Virginia 23228, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a special agent (SA) with the Federal Bureau of Investigation (FBI) and, as such, I am charged with enforcing all federal laws in all jurisdictions of the United States, its territories and possessions. I have been employed as an FBI SA since October 2014. Prior to being employed as an FBI SA, I was an FBI Computer Scientist from 2012 to 2014 and worked computer-enabled investigations. As an FBI SA I have received extensive training in the investigation of violations of federal and state law. I am currently assigned to the Richmond Division of the FBI where I investigate organized crime matters, which include computer-enabled criminal violations relating to bank fraud, identity fraud, and access device fraud. Based upon my training and experience, I am familiar with the means by which individuals obtain, reproduce, and

use access devices, namely debit and/or credit cards in support of various criminal offenses, and I have participated in the execution of numerous searches and seizures pursuant to warrants authorizing the seizure of evidence related to the bank fraud, identity fraud and access device fraud. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

RELEVANT STATUTORY PROVISIONS

3. Title 18, United States Code, Section 1029(a) (Fraud and related activity in connection with access devices), provides in pertinent part that:

(a) Whoever—

* * *

- (2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating \$1,000 or more during that period;
- (3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;
- (4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;
- (5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than \$1,000; or

* * *

shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) Section 1029.

4. Title 18, United States Code, Section 1028A (Aggravated identity theft), provides in pertinent part that whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

5. The following definitions apply to Sections 1028A and 1029:

- a. **“Access device”** means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);
- b. **“Unauthorized access device”** means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud;
- c. **“Produce”** includes design, alter, authenticate, duplicate, or assemble;
- d. **“Traffic”** means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of;
- e. **“Device-making equipment”** means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device;
- f. **“Means of identification”** means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any— (A) name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer

or taxpayer identification number; (B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (C) *unique electronic identification number*, address, or routing code; or (D) telecommunication identifying information or *access device* (emphasis added);

PROBABLE CAUSE

6. On or about March 3, 2018, I received a report from Henrico Federal Credit Union (HFCU) that a deep-insert payment card skimming device was installed on the HFCU automated teller machine (ATM) located at 9401 West Broad Street, Henrico, Virginia.

7. I responded to the location and observed a video recording device affixed to the top of the ATM. The recording device consisted of a metal piece of molding, in similar form and color of the ATM, and affixed to the top of the ATM using double-sided foam tape. I removed the recording device and observed a camera, circuit board, batteries, wires, and a microSD storage device attached to the underside of the recording device. The bottom side of the recording device had a pinhole positioned to allow the concealed camera to observe the ATM's keypad.

8. Skimming devices are used to fraudulently record the information stored on the magnetic stripe from payment cards, which includes card number, cardholder name, and other information necessary for financial transactions. The skimming devices are concealed deep inside the ATM card reader or placed in concealment devices on the external of the card reader. As victims used their payment cards at the ATM, the data contained on the magnetic stripe of the payment card is secretly recorded onto the skimming device. Once this information is captured, it is trivial to transfer the information on the card's magnetic stripe to another payment card that is

in the possession of an unauthorized individual with the use of a magnetic card encoder. In the case of the HFCU ATM, the skimming device was a flat piece of metal that was inserted deep into the card reader.

9. In order to use the payment card as a debit card, the personal identification number (PIN) associated with the card must be obtained. These PIN numbers are compromised using two basic strategies. The first approach, which involves a greater degree of effort and sophistication, is to compromise the PIN keypad itself using one or other technology that captures the victim's PIN as she enters it into the ATM's keypad. The second approach involves the perpetrator(s) placing a video recording device somewhere near the ATM with the camera focused on the keypad. The video recording device captures video of the victim typing their PIN on the keypad. In the case of the HFCU ATM, the perpetrators used the second approach, concealing a camera in a piece of plastic molding that they added to the top of the ATM.

10. I removed the microSD storage device from the video recording device and reviewed the files contained on the storage device. Several files contained video and audio recordings believed to be from the HFCU ATM and showed customers approaching the ATM, inserting their card into the ATM, and all keypresses made on the ATM keypad by the customer, including the customer's PINs.

11. One particular video on the microSD storage device from the video recording device showed what appeared to be a deep-insert skimming device being removed from the ATM at approximately March 3, 2018 at 9:55 am. The video captured the hands of an individual placing a flat, thin tool into the ATM card reader and pulling out a deep-insert skimming device. In order to disguise the activity, the individual removed a payment card from his wallet and walked away from the ATM with the payment card in hand. I reviewed the HFCU ATM video for the same time was reviewed, which captured the face and body of one of the subjects conducting the activity at the HFCU ATM.

12. Using various investigative techniques, the FBI developed information that the subjects possibly resided at the Park West End apartments, located at 5300 Glenside Drive, Henrico, Virginia. On March 8, 2018, at approximately 12:50 pm, an FBI surveillance team established surveillance near 5300 Glenside Drive, Building 18, Henrico, Virginia. The FBI observed two white males, both similar in appearance to the two subjects identified in HFCU ATM video installing the skimming device, leave a building located at 5300 Glenside Drive, Building 18, Henrico, Virginia, and enter the a 2017 Ford Edge bearing a New York license plate HSJ9730 ("VEHICLE 1").

13. Information obtained from the leasing office at the Park West End Apartment Complex indicates that Apartment 1808, otherwise known as the PREMISES, is leased to a "Luigi Latorza." A copy of the Italian passport that "Latorza" provided to the leasing office contained a photograph that appeared similar one of the subjects identified in the HFCU ATM video installing

the skimming device.

14. A review of Department of Motor Vehicles records reveals that VEHICLE 1 is registered to "PV Holdings Corp" and was described as a 2017 Ford "Edg," [sic] white in color, VIN 2FMPK4K9XHBC13295. PV Holdings Corporation is known to register vehicles used by Budget Rent A Car (Budget).

15. Information provided by Budget indicated that the VEHICLE 1 was rented for the period of February 28, 2018, through March 28, 2018, to Viorel Naboiu, who provided a Romanian driver's license, a Romanian address and U.S. telephone number 714-798-1891.

16. A record check conducted for the telephone number 714-798-1891 indicated that the telephone number is associated with the name "Luigi Latorza."

17. A check of records held by U.S. Immigration and Customs Enforcement (ICE) indicated that on or about June 12, 2015, Viorel Naboiu was detained by ICE. The booking photo of Viorel Naboiu appears to be the same subject as observed at the HFCU ATM surveillance video.

18. After reviewing photographs from the ICE booking photograph and the Italian passport photograph, I believe that "Luigi Latorza" is an alias for Viorel Naboiu. On March 15, 2018, at approximately 3:40 pm, the FBI established surveillance near 5300 Glenside Drive, Building 18, Henrico, Virginia. Surveillance team members observed one white male, similar in appearance to one of the subjects identified in HFCU ATM video who had installed the skimming device in the HFCU ATM, leave a building located at 5300 Glenside Drive, Building 18, Henrico, Virginia, and enter a second vehicle, described as a 2017 Mazda 6, red in color, Florida license

plate CIMB08 ("VEHICLE 2").

19. A review of Department of Motor Vehicles records reveals that VEHICLE 2 is registered to "PV Holdings Corp" and was rented by Budget on March 1, 2018, to Florin Bersanu. Bersanu provided Budget the address of 533 Glenside Drive, Richmond, Virginia, and telephone number (804) 401-2325.

20. During the course of the investigation, the FBI was contacted by a fraud investigator at Branch Banking and Trust ("BB&T") regarding a skimming event that occurred on February 28, 2018, at the BB&T branch located at 3214 Skipwith Road, Henrico, Virginia. On or about February 28, 2018, at 6:30 a.m., a skimming device was installed at the BB&T Skipwith Branch ATM and later removed at approximately 9:40 p.m. the same day. I reviewed the ATM surveillance camera recordings for the installation and removal timeframes and observed two males that appear to be Bersanu and Naboiu. Approximately 103 unique debit card numbers were transacted at the ATM between the installation and removal times.

21. Approximately 63 of the debit card numbers transacted at the Skipwith branch ATM between the installation and removal of the skimming device were used to conduct fraudulent ATM withdrawals at BB&T branch ATMs in the Richmond, Virginia area. BB&T provided photographs from several of the ATM surveillance cameras during the times of the fraudulent transactions and I observed two males conducting the ATM transactions. The males appear to be Bersanu and Naboiu.

22. On April 11, 2018, information obtained by the FBI revealed that Florin Bersanu rented a 2017 Toyota Corolla, gray in color, bearing Georgia license plate PPV-8512, from Enterprise located in Henrico, Virginia. The vehicle was rented for the period of April 11, 2018, 12:02 p.m. through May 11, 2018 10:00 a.m. On April 11, 2018, at approximately 5:30 p.m., I observed the above vehicle parked outside 5300 Glenside Drive, Building 18, Henrico, Virginia. Pursuant to a warrant issued in the Eastern District of Virginia, on or about April 13, 2018, a tracking device was installed on the Toyota Corolla.

23. The tracking device revealed that the vehicle was used from April 13 through April 14, 2018, to travel to, among other places, Ceredo, West Virginia, Hurricane, West Virginia and Dunbar, West Virginia. Based on the information from the tracking device, it appeared that the vehicle departed from 5300 Glenside Drive, Henrico, Virginia at approximately April 13, 2018, at 11:12 p.m. and arrived at United Bank's Ceredo branch, located at 555 C Street, Ceredo, West Virginia, at approximately 4:33 a.m. The ATM camera was obstructed by the individual at the ATM, however photographs from another surveillance camera showed a male, who appeared to be Naboiu, at the ATM machine at approximately 4:33 a.m.

24. On or about April 14, 2018, between 5:47 a.m. and 6:00 a.m., information from the tracking device indicated that the vehicle was in the vicinity of United Bank's Dunbar branch, located at 1200 Grosscup Avenue, Dunbar, West Virginia. The ATM camera was obstructed by the individual at the ATM and no other surveillance cameras were available.

25. On or about April 14, 2018, between 6:14 a.m. and 6:33 a.m., information from the tracking device indicated that the vehicle was in the vicinity of United Bank's Hurricane branch, located at 274 SR 34, Hurricane, West Virginia. Photographs from the ATM surveillance camera revealed a male that appeared to be Naboiu.

26. On or About April 14, 2018, between 6:45 a.m. and 6:49 a.m., information from the tracking device indicated that the vehicle was in the vicinity of United Bank's Dunbar branch. The ATM camera was obstructed by the individual at the ATM and no other surveillance cameras were available.

27. Information provided by the tracking device indicated that the vehicle arrived back at 5300 Glenside Drive, Henrico, Virginia, on or about April 14, 2018 at 11:18 a.m.

28. On or about April 15, 2018, FBI special agents from the Pittsburgh Division were requested to check the ATMs located at United Bank's Ceredo, Hurricane and Dunbar branches. Shortly thereafter, skimming devices were recovered from the ATMs at the Hurricane and Dunbar branches. Bank investigators provided the ATM logs for the Hurricane and Dunbar ATMs, which indicated that approximately 60 cards were captured from the Hurricane ATM and 28 cards were captured from the Dunbar ATM.

29. On or about April 15, 2018, information from the tracking device indicated that the vehicle departed 5300 Glenside Drive, Henrico, Virginia, at approximately April 15, 2018 at 12:57 p.m. and headed west towards West Virginia. At approximately 5:47 p.m., information from the tracking device indicated that the vehicle was in the vicinity of United Bank's Dunbar branch, and

at approximately 6:12 p.m. the vehicle was in the vicinity of United Bank's Hurricane branch. The vehicle then headed east and returned to the Henrico, Virginia area at approximately 11:05 p.m.

30. Based on my discussion with fraud investigators at both multiple financial institutions, investigators believe that these same subjects are involved in multiple ATM skimmer thefts that have resulted in the theft of at least 100 credit and debit card numbers (*i.e.*, "access devices") in the Richmond metro area, approximately 60 access devices from two BB&T banks in Newport News, approximately 87 access devices from United Banks in West Virginia, 235 access devices from Pen Air Federal Credit Union in Pensacola, Florida, and 226 access devices from Eglin Federal Credit Union in Mary Esther, Florida. BB&T investigators further suspect these same subjects are involved in multiple incidents in Maryland. Investigators base this conclusion on review of ATM surveillance photos as well as similarities in the exploits used to steal the access device numbers.

UNLOCKING ELECTRONIC DEVICES USING BIOMETRIC FEATURES

31. Through my experience investigating these types of matters, I have learned that subjects committing access device fraud using ATM skimmer devices are often associated with sophisticated organized crime groups. Investigators commonly see such groups using applications on their mobile devices to send and receive encrypted messages, in both text and voice formats, during the planning and execution of their criminal conduct. Wickr, WhatsApp, Signal, and Telegram are a few examples of mobile applications that allow end-to-end encrypted communication, and as such, are typically beyond the abilities of law enforcement agencies to

wiretap. According to the Wickr website, Wickr uses end-to-end encryption, and the “content is encrypted locally on user devices and is only accessible to intended recipients.”

32. Several of these secure messaging applications provide an option to set a self-destruct date for messages. Wickr, for example, advertises that messages are ephemeral, and “no conversation lives beyond its useful life – you decide when your content gets automatically deleted for good.” The suspects and their conspirers may choose to place an expiration date on the messages, where at such a time the secure messaging application automatically and irrevocably deletes the conversation from the mobile device. Such deleted conversations cannot be recovered using even the most sophisticated forensic tools available to law enforcement. Wickr also uses an “require authentication” setting that, when enabled, requires the user to enter their Wickr password each time the application is used. If the “require authentication” setting is disabled, Wickr will not prompt for the Wickr password for a short amount of time after the last successful use of the Wickr password, allowing law enforcement a short window in order to access messages sent and/or received using the Wickr application. Wickr is not alone in this capability: the other messaging applications operate in a similar manner.

33. Through my experience with a previous investigation involving access device fraud, I observed subjects use multiple mobile devices to communicate with other members of their organization. Substantial communications discussing criminal acts did not occur via email or text message, but rather through the use of encrypted messaging applications, such as the applications mentioned above. At the time of arrest, investigators observed messages with

expiration dates within the Wickr application. However, by the time a forensic examination was conducted, the messages had been erased and were unable to be recovered. In order to preserve these time-sensitive messages, it is essential that investigators be able to access a mobile device immediately.

34. I know from my training and experience, as well as publicly available materials, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

35. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. Examples of such devices providing a fingerprint unlocking capability are several models of Apple's iPhone, as well as several phones, including but not limited to the Samsung Galaxy, which use the Android operating system. Apple iPhones may be fingerprint unlocked using a function called Touch ID, which during setup allows for registering as many as five (5) fingerprints to unlock the device. Samsung's Galaxy S8 and S8+ models may be configured to be unlocked with as many as four (4) fingerprints. In fact, the number of electronic devices providing a fingerprint unlocking capability, including both smart phones and laptops, is growing continually.

36. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based upon the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

37. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

38. In my training and experience, users of electronic devices often enable the above-mentioned biometric features because they are considered a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. In some instances, biometric features are considered a more secure way to protect a device's contents. This is

particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

39. As discussed in this affidavit, my training and experience leads me to believe that investigators are likely to find one or more digital devices during the search. The passcode or password that would unlock any such device subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

40. Biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: 1) more than 48 hours has elapsed since the device was last unlocked; or 2) when the device has not been unlocked using a fingerprint for eight (8) hours *and* the passcode or password has not been entered in the last six (6) days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four (4) hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

41. I have also learned through my training and experience that while the person who is in possession of a device, or has the device among his or her belongings at the time the device

is found, is likely a user of the device, that person may *not* be the *only* user of that device whose fingerprints are among those that will unlock it. It is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a PREMISES without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the PREMISES who law enforcement officials reasonably believe to be a user of the device to unlock the device using biometric features in the same manner as discussed above.

42. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of these biometric features, the warrant I am applying for would permit law enforcement personnel to: 1) press or swipe the fingers (including thumbs) of any individual, who is found at the PREMISES and reasonably believed by law enforcement to be a user of the device(s), to the fingerprint scanner of the device(s) found at the PREMISES; 2) hold the device(s) found at the PREMISES in front of the face of those same individuals and activate the facial recognition feature; and/or 3) hold the device(s) found at the PREMISES in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant. In the event that law enforcement is unable to unlock any cellphone found in the PREMISES within the number of attempts permitted by the pertinent

operating system, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

43. Due to the foregoing, I request that the Court authorize law enforcement personnel to press the fingers (including thumbs) of individuals found at the PREMISES to the fingerprint sensor of any such device found at the PREMISES in an attempt to unlock the device and search its contents as authorized by this warrant.

TECHNICAL TERMS

44. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections

between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

45. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

46. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a

computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases conceivably ever.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

47. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant

at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of

counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

- f. I know that when an individual uses a computer to commit identity theft, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

48. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is

true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be

stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

49. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

50. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

SPECIFICITY OF SEARCH WARRANT RETURN

51. Consistent with the Court's current policy, the search warrant return will list the model(s) and serial number(s) of any and all computers seized at the SUBJECT PREMISES, and include a general description of any and all associated peripheral equipment that has been seized. Additionally, the search warrant return will include the total numbers of each type of digital media that has been seized (e.g., "ten (10) 3.5" diskettes; twenty (20) CDs; twenty (20) DVDs; three (3)

USB drives; one (1) 256 MB flash memory card,” *etc.*)

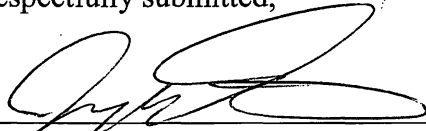
NOTICE REGARDING INITIATION OF FORENSIC EXAMINATION

52. Moreover, the Government will file a written pleading in this case within one hundred twenty (120) days after the execution of the search warrant notifying the court that the imaging process of digital evidence seized from the target location is complete, and the forensic analysis of computers and media has begun. Such notice will include confirmation that written notice has been provided to the defendant or his counsel informing the defendant that the forensic examination of evidence seized from him has actually begun. Such notice to the defendant and the Court is not intended to mean, and should not be construed to mean, that the forensic analysis is complete, or that a written report detailing the results of the examination to date will be filed with the Court or provided to the defendant or his counsel. This notice does not create, and is not meant to create, additional discovery rights for the defendant. Rather, the sole purpose of this notice is to notify the defendant that, beyond the simple seizure of his property, a forensic search of that property has actually begun.

CONCLUSION

53. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,



Jeremy A. D'Errico
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on May 7, 2018:

/s/



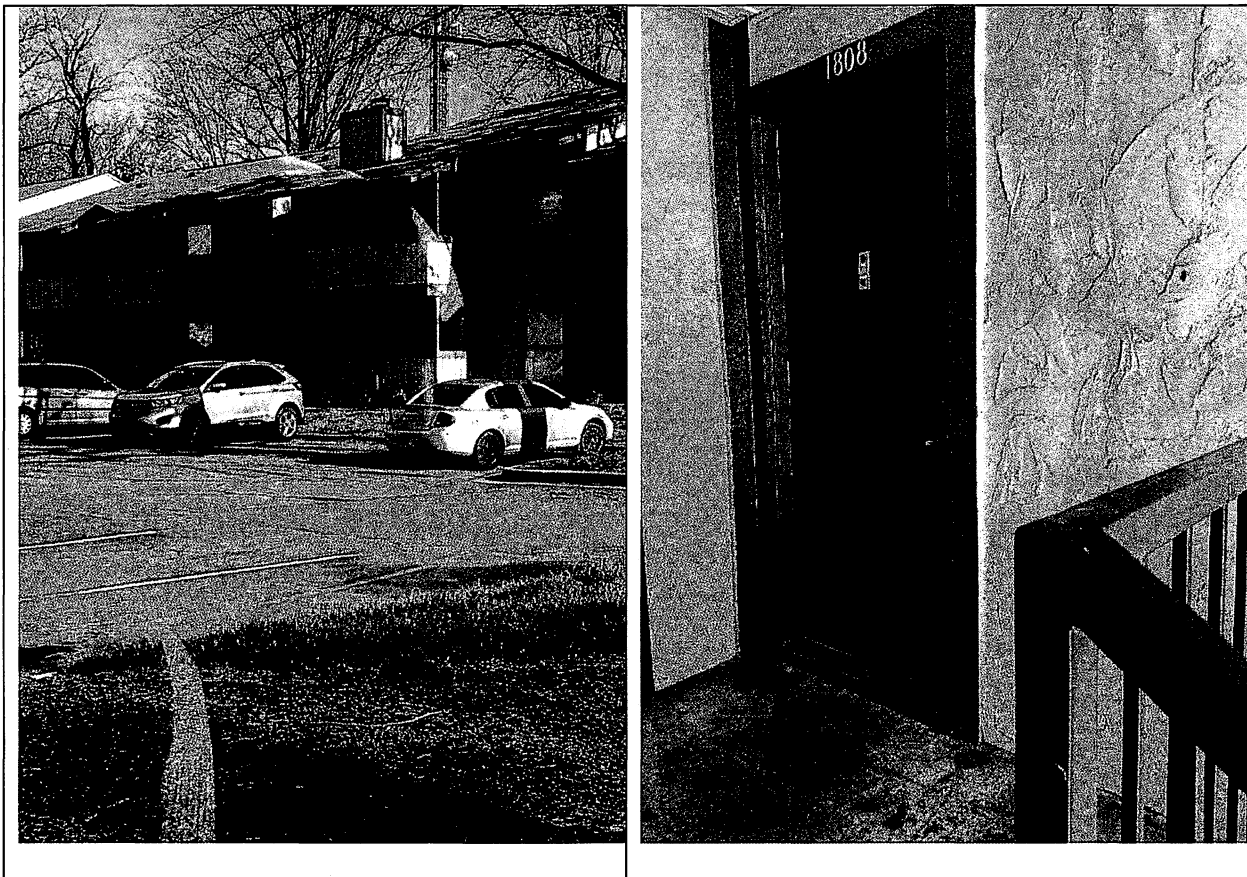
David J. Novak
United States Magistrate Judge

ATTACHMENT A

Property to be Searched

The property to be searched is 5300 Glenside Drive, Apartment 1808, Henrico, Virginia (“PREMISES”).

The PREMISES are further described as an apartment unit located on the second floor of building 18. The apartment unit 1808 has a black door with gray molding and the numbers “1808” posted in white above the door. From the front of the building, the apartment is located at the top of the left-most stairwell and is the first door on the right.



ATTACHMENT B

Property to be Seized

1. All records relating to violations of 18 U.S.C § 1028A relating to aggravated identity theft and 18 U.S.C. § 1029 relating to fraud and related activity in connection with access devices, including:
 - a. skimming devices and components of skimming devices including, cameras, charging devices, cables, batteries, circuit boards, integrated circuits, thin pieces of plastic or metal, keypad covers or other related items, including correspondence, orders, invoices and/or receipts for these items;
 - b. tools, equipment, and instructions used to manufacture or install skimming devices, such as screw drivers, soldering irons, solder, double-sided tape, molding, paint, pant samples, tin snips, knives, or cutting implements, and including correspondence, orders, invoices and/or receipts for these items;
 - c. items used to create payment cards, such as magnetic card reader/encoders, computers, cards containing magnetic stripes (with or without cardholder information printed/embossed), embossers, tippers, or encoding software, including correspondence, orders, invoices and/or receipts for these items;
 - d. records and information relating to the obtaining, possession, concealment, or transfer of U.S. or foreign currency, including bank records, ATM receipts, money transfer receipts or orders, cashier's checks or receipts, bank drafts, bank checks, prepaid cards, debit cards, payment cards, safe deposit box keys or other similar items;

- e. records and information relating to travel and residence, including lodging, lease agreements, rental vehicles, airline bookings, flights, GPS data from navigation systems, mailing addresses, PO boxes, or similar items;
- f. records and information relating to the conspiracy to defraud financial institutions;
- g. records and information relating to the identity or location of the suspects; and
- h. records and information relating to software used to create or use access devices
- i. any and all “access devices,” as that term is defined in 18 U.S.C. § 1029, and “means of identification,” as that term is defined in 18 U.S.C. § 1028.

2. Computers or storage media used as a means to commit the violations described above, including in the creation or storage of access devices in violation of 18 U.S.C. § 1029.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious

software;

- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.

4. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form

(such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

6. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

7. *During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are authorized to: 1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device(s) found at the premises; 2) hold the device(s) found at the premises in front of the face those same individuals and activate the facial recognition feature; and/or 3) hold the device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.*